Jurnal Hukum dan Etika Kesehatan 6 (1), Maret 2026
E-ISSN : 2798-043X
Research Article
DOI : 10.30649/jhek.v6i1.270

PERLINDUNGAN HUKUM DATA KESEHATAN PASIEN DI ERA DIGITAL

LEGAL PROTECTION OF PATIENTS' HEALTH DATA IN THE DIGITAL ERA

Yessy Andriani Fauziah[1], Dany Agus Susanto[2], Yudhistira Prawira Utama[3*]
[1] School of Dental Medicine, Universitas Ciputra, Surabaya
[2,3] Fakultas Hukum, Universitas 45, Surabaya
[*] Correspondence : yessy.andriani@ciputra.ac.id

Received : 19 Oktober 2025 Accepted : 2 Februari 2026
Revised : 2 Februari 2026 Published : 3 Februari 2026

Abstrak

Transformasi digital di bidang kesehatan mempercepat pertukaran data lintas platform, tetapi juga meningkatkan risiko pelanggaran privasi dan kebocoran informasi pasien. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan mempertegas pentingnya tata kelola data medis yang aman dan akuntabel. Artikel ini bertujuan menganalisis kecukupan perlindungan hukum terhadap data kesehatan pasien di Indonesia, khususnya koherensi dan celah hukum (*normative gap*) dalam penerapan kedua undang-undang tersebut serta hubungannya dengan prinsip etika kedokteran. Metode penelitian menggunakan penelitian hukum normatif dengan menggunakan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan perbandingan. Hasil menunjukkan bahwa meskipun telah diatur secara eksplisit dalam regulasi, masih terdapat celah terkait standar keamanan, interoperabilitas, dan kualitas persetujuan digital. Kajian ini merekomendasikan penerapan *Data Protection Impact Assessment* (DPIA), audit independen, dan integrasi etika digital dalam pendidikan tenaga kesehatan guna memperkuat akuntabilitas dan menjaga kepercayaan publik seperti halnya yang telah dilakukan oleh Uni Eropa dan Amerika Serikat melalui regulasi-regulasi yang telah kedua negara tersebut berlakukan.
Kata Kunci : Perlindungan hukum; Data kesehatan; Etika kedokteran; Era digital

Abstract

Digital transformation in the health sector has accelerated cross platform data exchange, while at the same time increasing the risks of privacy violations and patient information leakage. Law Number 27 of 2022 on Personal Data Protection and Law Number 17 of 2023 on Health emphasize the importance of secure and accountable medical data governance in Indonesia. This article aims to analyze the adequacy of legal protection for patient health data, with particular

attention to regulatory coherence and existing normative gaps in the implementation of these two laws, as well as their relationship with the principles of medical ethics. This study applies a normative legal research method using a statutory approach, a conceptual approach, and a comparative approach. The statutory approach examines relevant legislation governing health data protection, while the conceptual approach explores ethical principles such as patient autonomy, confidentiality, and accountability. The comparative approach draws lessons from international regulatory practices to provide broader context. The findings indicate that although patient health data protection is explicitly regulated, significant gaps remain in practice, particularly regarding security standards, system interoperability, and the quality of digital consent. These weaknesses may undermine patient trust and increase legal and ethical risks. Therefore, this study recommends the implementation of Data Protection Impact Assessments, independent audits, and the integration of digital ethics into health professional education to strengthen accountability and sustain public trust, following best practices adopted in the European Union and the United States.

Keywords : *Legal protection; Health data; Medical ethics; Digital era.*

Pendahuluan

Transformasi layanan kesehatan di era digital mendorong peralihan dari sistem analog ke ekosistem terhubung berbasis rekam medis elektronik, aplikasi kesehatan, analitik data, dan integrasi lintas fasilitas. Perubahan ini meningkatkan akses dan efisiensi pengambilan keputusan klinis, namun sekaligus memunculkan tantangan serius terkait privasi, kerahasiaan, dan akuntabilitas tata kelola data sebagaimana ditandai dalam literatur pascapandemi (Keesara et al., 2020). Era digital membawa perubahan signifikan pada sistem pelayanan kesehatan melalui penerapan rekam medis elektronik, telehealth, serta integrasi lintas fasilitas. Namun, di balik manfaat efisiensi dan aksesibilitas, muncul tantangan hukum dan etik terkait privasi pasien, kerahasiaan informasi, dan akuntabilitas pengendali data. Kasus kebocoran data pasien, seperti penyebaran rekam medis laboratorium, data BPJS Kesehatan, dan hasil radiografi di cloud publik, memperlihatkan lemahnya kontrol keamanan dan pengawasan hukum terhadap data pribadi di sektor kesehatan (Nusantara et al., 2024). Pelanggaran ini tidak hanya melanggar hak privasi, tetapi juga berpotensi menimbulkan diskriminasi sosial dan ekonomi bagi pasien.

Dalam penerapan layanan kesehatan, penggunaan teknologi jarak jauh dan perangkat digital memunculkan berbagai isu etik dan hukum, seperti keabsahan persetujuan, perlindungan data pribadi, tanggung jawab profesional, hingga standar keamanan informasi (Fauziah, Agustin Wahjuningrum, et al., 2024). Kajian terkini menunjukkan bahwa rancangan layanan sering kali belum menempatkan pasien sebagai pemilik data yang berdaulat, sehingga terjadi ketimpangan informasi antara pasien dan penyedia layanan kesehatan (Solimini et al., 2021).

Ancaman keamanan data kesehatan semakin kompleks, dengan rumah sakit dan platform layanan kesehatan rentan terhadap *phishing*, *ransomware*, kesalahan konfigurasi *cloud*, serta penyalahgunaan akses internal. Perlindungan yang hanya bersifat teknis tidak memadai, diperlukan tata kelola organisasi yang terpadu dan berkelanjutan.

Pengalaman negara-negara Asia dan Eropa menunjukkan pentingnya mekanisme yang transparan, dapat diaudit, dan selaras dengan prinsip perlindungan data modern. Tanpa penerapan *privacy by design* sejak awal, risiko pelebaran tujuan pemrosesan (*function creep*) dan pengungkapan kembali identitas pasien (*re-identification*) akan meningkat (Jungkunz et al., 2021).

Di Indonesia, perubahan hukum penting terjadi melalui Undang-Undang Pelindungan Data Pribadi (2022) dan Undang-Undang Kesehatan (2023), yang mempertegas kekhususan data kesehatan serta mengatur penyelenggaraan rekam medis elektronik. Namun, literatur kebijakan menunjukkan bahwa implementasi sering tidak merata dan membutuhkan kepemimpinan organisasi serta budaya kepatuhan yang kuat (Fauziah, Alhadad, et al., 2025). Perlindungan hukum terhadap data kesehatan menjadi isu penting, terutama setelah lahirnya dua regulasi yang saling berkaitan tentang data kesehatan pasien, yaitu: UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan UU No. 17 Tahun 2023 tentang Kesehatan (UU Kesehatan). Keduanya mengatur prinsip dasar privasi, namun implementasinya masih menyisakan ketimpangan antara norma hukum dan praktik teknis di fasilitas layanan kesehatan.

Aspek bioetika menekankan otonomi pasien untuk memahami tujuan pengumpulan data, pihak yang mengakses, jangka waktu penyimpanan, serta hak menarik persetujuan, sementara prinsip kemanfaatan dan tidak merugikan menuntut agar pemanfaatan data berorientasi pada kepentingan pasien dan menghindari risiko seperti kebocoran data pribadi. Hal yang pernah terjadi seperti kebocoran data BPJS Kesehatan pada tahun 2021 perlu diantisipasi, mengingat data yang diduga bocor tersebut memuat informasi pribadi yang sangat sensitif, antara lain Nomor Induk Kependudukan (NIK), nama lengkap, alamat domisili, email, nomor telepon, hingga data lain seperti gaji dan potensi riwayat kesehatan**.** Laporan hasil investigasi Kementerian Komunikasi dan Informatika menyebutkan bahwa dataset yang beredar secara daring memiliki kemiripan kuat dengan data peserta BPJS Kesehatan dan mencakup NIK, alamat, email, nomor telepon, serta gaji (Kompas.com. 2021, Mei 21). Data dalam basis data BPJS Kesehatan bersifat sangat pribadi dan rentan disalahgunakan, sehingga prinsip keadilan menuntut perlindungan setara bagi seluruh pasien dengan pemanfaatan data yang dibatasi secara jelas untuk kepentingan layanan, audit, pendidikan, dan penelitian melalui prinsip minimisasi, anonimisasi, persetujuan sah dan terinformasi, serta pengaturan ketat penggunaan sekunder agar tetap menghormati hak pasien (Nusantara et al., 2024).

Di wilayah penggunaan data pribadi pasien yang dipergunakan untuk riset dan pengembangan AI (*Artificial Intelligence*), isu legitimasi dan akuntabilitas menjadi perdebatan. Penggunaan data di luar layanan klinis langsung harus didasari tujuan yang spesifik, dokumentasi yang transparan, dan pengawasan yang independen (Fauziah, Alhadad, et al., 2024). Penelitian lintas yurisdiksi memperlihatkan pentingnya menetapkan dasar hukum yang tepat, menerapkan minimisasi data, dan menyediakan jalur audit yang memungkinkan penelusuran keputusan saat terjadi dampak merugikan

bagi pasien (Ho, 2024).

Isu interoperabilitas turut menentukan mutu dan keselamatan layanan. Pertukaran data yang aman antar fasilitas mempercepat rujukan dan menghindari pengulangan pemeriksaan, tetapi tanpa standar yang seragam dan kontrol keamanan yang memadai, risiko kebocoran meningkat (E. Li et al., 2022). Penetapan peran dan tanggung jawab antara pengendali dan pemroses data harus tegas dalam kontrak pemrosesan, yang idealnya memuat standar teknis dan organisasional, hak audit, lokasi dan retensi data, pengelolaan kunci, keterlibatan sub-pemroses, serta tenggat pelaporan insiden (Z. Li et al., 2023).

Penilaian Dampak Perlindungan Data (DPIA) perlu diterapkan di layanan kesehatan untuk pemrosesan berisiko tinggi seperti integrasi data skala besar atau pelatihan model AI pada citra radiograf, karena DPIA berfungsi memetakan risiko, menetapkan mitigasi yang proporsional, dan mendokumentasikan akuntabilitas yang dapat diaudit sebagai jembatan antara prinsip hukum-etika dan praktik (Ali & Osmanaj, 2020). Dari sudut pandang keseimbangan manfaat dan risiko, penggunaan data untuk audit mutu, pendidikan, dan penelitian harus tunduk pada minimisasi, *pseudonymization* atau *de-identification*, serta pengawasan komite etik (Darmadi et al., 2025).

Kesenjangan kapasitas institusional rumah sakit besar dan fasilitas layanan primer mendorong kebutuhan panduan operasional yang sederhana namun tegas, serta skema dukungan teknis. Berangkat dari keseluruhan gambaran, penelitian ini diperlukan untuk menjembatani nilai etika, kerangka regulasi, dan praktik klinis yang sering kali berjalan masing-masing (Keesara et al., 2020).

Berdasarkan uraian di atas, maka penulis menarik rumusan sebagai berikut:

1. Bagaimana pengaturan perlindungan data pribadi pasien yang telah dilakukan di luar negeri?
2. Bagaimana pengaturan perlindungan data pribadi pasien dalam dunia kesehatan di Indonesia?

Kajian ini bertujuan menjelaskan perlindungan data pribadi pasien serta mendorong klinik dan rumah sakit menerapkan standar operasional yang jelas, mudah diterapkan, dan diawasi secara ketat agar mencegah penyalahgunaan atau kebocoran data, meningkatkan kepercayaan pasien, dan mendukung mutu layanan.

Metode Penelitian

Kajian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan perbandingan (*comparative approach*). Pendekatan perundang-undangan dilakukan dengan menelaah dan menafsirkan perangkat regulasi yang relevan, terutama UU PDP, UU Kesehatan, serta Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis Elektronik. Pendekatan konseptual digunakan untuk mengkaji prinsip etika kedokteran yang berkaitan dengan kerahasiaan, otonomi, kemanfaatan, tidak merugikan, dan keadilan, serta konsep akuntabilitas pengendali dan pemroses data dalam ekosistem layanan kesehatan digital. Pendekatan perbandingan

digunakan untuk mengetahui standar perlindungan data pribadi pasien yang telah dilakukan di beberapa negara.

Analisis dan Diskusi

A. Peraturan Perlindungan Data Pribadi Pasien di Beberapa Negara

Dalam mengkaji suatu permasalahan hukum bilamana dalam penerapan peraturan di Indonesia masih terdapat suatu problematika hukum seperti halnya dalam penulisan ini, digunakan metode penelitian hukum normatif dengan menggunakan beberapa pendekatan seperti yang dijelaskan sebelumnya. Salah satu pendekatan yang digunakan dalam penulisan ini adalah dengan menggunakan metode pendekatan perbandingan (*comparative approach*), di mana metode pendekatan ini untuk menunjukkan beberapa peraturan yang telah dilaksanakan dibeberapa negara terkait Perlindungan Data Pribadi Pasien. Beberapa peraturan diberbagai negara antara lain:

A.1. *General Data Protection Regulation* (*GDPR*) di Uni Eropa

General Data Protection Regulation (GDPR) berlaku sejak 25 Mei 2018, merupakan regulasi Uni Eropa dengan standar perlindungan data yang sangat ketat dan berlaku secara ekstrateritorial bagi setiap organisasi yang memproses data pribadi warga Uni Eropa, dengan penegakan tegas melalui sanksi denda tinggi terhadap pelanggaran privasi dan keamanan data. *GDPR* ini memberikan beberapa definisi terkait data pribadi, antara lain:

1. Data Pribadi, adalah berbagai informasi yang berkaitan dengan individu yang dapat diidentifikasi secara langsung atau tidak langsung. Baik itu nama dan alamat email dianggap merupakan data rpibadi. Informasi terkait lokasi terkini, etnis, jenis kelamin, data biometrik, keyakinan agama, cookie web, dan opini dalam dunia politik juga dianggap oleh *GDPR* sebagai data pribadi.
2. Pemrosesan data, adalah setiap tindakan yang dilakukan pada data, baik otomatis maupun manual, termasuk pengumpulan, pencatatan, pengorganisasian, penataan, penyimpanan, penggunaan, penghapusan, dan lain sebagainya yang pada dasarnya terkait informasi yang mampu memgidentifikasi seseorang dianggap sebagai pemrosesan data.
3. Subjek data, adalah orang yang datanya pribadinya diproses. Baik ini pelanggan atau pengunjung situs yang mana datanya tersebut dan terekam dalam dunia digital.
4. Pengontrol data, adalah orang yang memutuskan mengapa dan bagaimana data pribadi akan diproses. Jadi pengontrol data adalah pemilik atau karyawan di suatu organisasi yang bertugas untuk mengelola dan meproses data pribadi seseorang yang sudah terekam dalam organisasi anda.
5. Pengolah data, adalah pihak ketiga yang memproses data pribadi atas nama pengontrol data. *GDPR* memiliki aturan khusus untuk individu dan

organisasi terkait pengolah data pribadi seseorang. Ini dapat mencakup server cloud seperti Google Drive, Proton Drive, atau Microsoft OneDrive, atau penyedia layanan email seperti Gmail atau Proton Mail.

Jika suatu organisasi ingin memproses suatu data pribadi seseorang, maka *GDPR* memberikan beberapa prinsip yang harus dijalankan sebagai upaya memberikan Perlindungan Data Pribadi seseorang, antara lain:

1. Kepatuhan hukum, keadilan, dan transparansi.
   Pemrosesan data pribadi harus sah, adil, dan transparan bagi subjek data
2. Pembatasan tujuan
   Dalam melakukan pemrosesan data harus jelas, spesifik dan sah dipergunakan untuk apa data dari subjek data yang akan dikumpulkan tersebut.
3. Minimalisasi data
   Pengumpulan dan pemrosesan data hanya sebatas hal-hal yang benar-benar diperlukan untuk tujuan yang dimaksud.
4. Keakuratan
   Data pribadi yang dikumpulkan dan diproses harus benar-benar dijaga keakuratan dan kemutakhiran datanya.
5. Pembatasan penyimpanan
   Data pribadi yang dikumpulkan dan diproses hanya boleh disimpan selama diperlukan untuk tujuan yang ditentukan.
6. Integritas dan kerahasiaan
   Pemrosesan harus dilakukan sedemikian rupa untuk memastikan keamanan, integritas, dan kerahasiaan yang sesuai (misalnya dengan menggunakan enkripsi)
7. Akuntabilitas
   Pengontrol data bertanggung jawab untuk dapat menunjukkan kepatuhan terhadap *GDPR* dengan semua prinsip ini.

GDPR mengakui sejumlah hak privasi baru bagi subjek data, yang bertujuan untuk memberikan individu lebih banyak kendali atas data yang mereka berikan kepada organisasi pengumpul, pengolah, dan pemroses data. Berikut adalah Hak Privasi subjek data yang diatur oleh *GDPR*, antara lain:

1. Hak untuk diinformasikan;
2. Hak akses;
3. Hak untuk perbaikan;
4. Hak untuk penghapusan;
5. Hak untuk membatasi pemrosesan;
6. Hak untuk portabilitas data;
7. Hak untuk keberatan; dan
8. Hak terkait pengambilan keputusan otomatis dan pembuatan profil.

A.2. *Health Insurance Portability and Accountability Act* (*HIPAA*) di Amerika Serikat

Health Insurance Portability and Accountability Act (*HIPAA*) merupakan aturan yang diberlakukan di Amerika Serikat (AS) yang bertujuan untuk melindungi privasi pasien dan mengamankan informasi kesehatan. HIPAA menetapkan standar ketat bagi penyedia layanan kesehatan dan pihak terkait dalam mengelola, mentransmisikan, dan menyimpan informasi kesehatan yang dilindungi guna mencegah akses tidak sah, menjamin kerahasiaan, serta memperkuat kepercayaan pasien terhadap sistem pelayanan kesehatan. HIPAA menetapkan standar federal untuk melindungi keamanan informasi kesehatan elektronik (*electronic Protect Health Information* atau ePHI) guna menjamin kerahasiaan, integritas, dan ketersediaannya, sekaligus memungkinkan akses sah bagi pihak terkait dalam mendukung kesinambungan perawatan, dengan pengaturan yang mencakup aturan privasi dan keamanan, kewajiban pelaporan pelanggaran, serta edukasi profesional kesehatan agar kepatuhan hukum dan kepercayaan pasien tetap terjaga dalam praktik layanan sehari-hari.

HIPAA terdiri dari 5 bagian yang menjadi fokus pengaturannya, antara lain:

1. Fokus pada akses, portabilitas, dan pembaharuan layanan kesehatan;
2. Pencegahan penipuan dan penyalahgunaan layanan kesehatan, penyerdahanaan administrasi, dan reformasi tanggungjawab medis;
3. Ketentuan kesehatan terkait pajak yang mengatur tabungan medis;
4. Penerapan dan penegakan persyaratan asuransi kesehatan kelompok;
5. Pengurangan pajak yang mengatur pengurangan pendapatan untuk pemberi kerja.

B. Pengaturan Perlindungan Data Pribadi Pasien di Indonesia

B.1. Peraturan-Peraturan tentang Perlindungan Data Pribadi Pasien di Indonesia

Tata kelola data kesehatan di Indonesia bertumpu pada tiga pilar utama, yaitu UU PDP sebagai regulasi umum, UU Kesehatan sebagai dasar hukum sektor kesehatan, dan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis (Permenkes 24/2022) yang mengatur aspek teknis Rekam Medis Elektronik. Ketiga regulasi tersebut saling melengkapi dalam membangun sistem pengelolaan data kesehatan yang terstandar, aman, transparan, dan berkeadilan.

UU PDP memberikan pengaturan yang masih luas dan umum terkait perlidungan data pribadi. Dalam Pasal 4 ayat (1) UU PDP menyatakan bahwa ada dua Jenis data pribadi yang diatur dalam UU PDP, yaitu: 1) Data Pribadi yang bersifat spesifik; dan 2) Data Pribadi yang bersifat umum. Selanjutnya dalam penjelasan Pasal 4 ayat (1) ini dijelaskan bahwa Data Pribadi yang bersifat spesifik ini adalah data pribadi yang dalam pemrosesannya dapat mengakibatkan dampak lebih besar kepada subjek data pribadi, dampak tersebut dapat berupa tindakan diskriminasi dan dapat menimbulkan kerugian yang lebih besar kepada subjek data pribadi tersebut. Sedangkan data yang bersifat umum merupakan jenis data pribadi yang secara umum dapa diidentifikasi oleh banyak orang.

Data pribadi yang bersifat spesifik, diatur lebih lanjut dalam ayat (2) Pasal 4 UU

PDP, yaitu:

a. Data informasi kesehatan;
b. Data biometrik;
c. Data genetika;
d. Catatan kriminal;
e. Data anak;
f. Data keuangan pribadi; dan/atau
g. Data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

Terlihat dalam Pasal 4 ayat (2) di atas, UU PDP sebenarnya juga mengatur terkait data informasi kesehatan subjek data pribadi. Namun hak-hak yang dilindungi dalam UU PDP ini masih melindungi hak subjek data pribadi secara umum. Hal ini dijelaskan dalam BAB IV UU PDP yang diatur dalam Pasal 5 sampai Pasal 15 UU PDP. Adapun hak-hak subjek data pribadi yang dilindungi oleh UU PDP dalam BAB IV yaitu:

a. Berhak mendapatkan informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, dan akuntabilitas pihak yang meminta data pribadi; (Pasal 5)
b. Berhak melengkapi, memperbaharui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi tentang dirinya sesuai dengan tujuan pemrosesan data pribadi; (Pasal 6)
c. Berhak mendapatkan akses dan memperoleh salinan data pribadi tentang dirinya; (Pasal 7)
d. Berhak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi tentang dirinya; (Pasal 8)
e. Berhak menarik kembali persetujuan pemrosesan data pribadi tentang dirinya yang telah diberikan kepada pengendali data pribadi; (Pasal 9)
f. Berhak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis, termasuk pemrofilan, yang menimbulkan akibat hukum atau berdampak signifikan pada subjek data pribadi; (Pasal 10 ayat (1))
g. Berhak menunda atau membatasi pemrosesan data pribadi secara proposional sesuai dengan tujuan pemrosesan data pribadi; (Pasal 11)
h. Berhak menggugat dan menerima ganti rugi atas pelanggaran tentang dirinya; (Pasal 12 ayat (1))
i. Berhak mendapatkan dan/atau menggunakan data pribadi tentang dirinya dari pengendali data pribadi dalam bentuk yang sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik; (Pasal 13 ayat (1))

UU PDP memberikan hak yang lebih luas bagi pasien sebagai subjek data, seperti hak untuk mengakses, memperbaiki, menghapus, dan menarik persetujuan atas data pribadi mereka. Selain itu juga, UU PDP juga memperluas pengaturan ke seluruh sektor, termasuk kesehatan, dengan memperkenalkan prinsip-prinsip dasar seperti *lawfulness,*

fairness, transparency, purpose limitation, dan data minimization. Dalam konteks layanan kesehatan, undang-undang ini menegaskan bahwa pengumpulan dan pemrosesan data kesehatan hanya boleh dilakukan untuk tujuan yang sah, jelas, dan sesuai dengan persetujuan pasien. Dalam Pasal 16 ayat (2) UU PDP menjelaskan:

> "Pemrosesan Data Pribadi harus dilakukan dengan prinsip Perlindungan Data Pribadi, meliputi:
>
> a. Data pribadi dikumpulan secara terbatas dan spesifik, sah secara hukum, dan transparan;
> b. Data pribadi harus diproses secara jelas sesuai dengan tujuannya;
> c. Memberikan jaminan terhadap hak subjek data pribadi dalam melakukan pemrosesan;
> d. Pemrosesan harus dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan;
> e. Pemrosesan data pribadi harus melindungi keamanan data pribadi dari pengaksesan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusaka, dan/atau penghilangan data pribadi;
> f. Pemrosesan data pribadi dilakukan dengan memberitahukan tujuan dan aktifitas pemrosesan, serta kegagalan perlindungan data pribadi;
> g. Data pribadi harus segera dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan subjek data pribadi;
> h. Pemrosesan data pribadi dilakukan secara bertanggungjawab dan dapat dibuktikan secara jelas.

Pengendali data seperti rumah sakit atau penyedia platform telemedisin, wajib menerapkan langkah-langkah keamanan yang memadai dan melaporkan setiap pelanggaran data kepada otoritas berwenang. Selain itu juga pengendali data pribadi juga harus memiliki dasar dan/atau alasan dalam melakukan pemrosesan data pribadi, seperti yang diatur dalam Pasal 20 ayat (1) UU PDP. Pengendali data pribadi juga harus menyampaikan berbagai informasi yang terkait dengan pemrosesan data pribadi tersebut seperti, legalitas, tujuan, jenis dan relevansi, jangka waktu retensi, rincian informasi yang akan dikumpulkan, dan hak-hak dari subjek data pribadi (Pasal 21 ayat (1) UU PDP).

UU Kesehatan menempatkan perlindungan data pribadi sebagai bagian dari hak pasien dan kewajiban tenaga kesehatan. Dalam Pasal 4 ayat (1) UU Kesehatan dijelaskan bahwa setiap orang berhak untuk memperoleh kerahasiaan data dan informasi kesehatan pribadinya. Setiap fasilitas pelayanan kesehatan wajib menjaga kerahasiaan informasi yang diperoleh selama proses pelayanan, termasuk hasil pemeriksaan laboratorium, citra radiologi, dan catatan terapi. Namun prinsip kerahasiaan tersebut tidak berlaku atau ada pengecualian dalam hal sebagaimana diatur dalam Pasal 4 ayat (4) UU Kesehatan, yaitu dalam hal-hal sebagai berikut:

> a. Pemenuhan permintaan aparat penegak hukum dalam rangka penegakan hukum;

b. Penanggulangan KLB, Wabah, atau bencana;
c. Kepentingan pendidikan dan penelitian secara terbata;
d. Upaya perlindungan terhadap bahaya ancaman keselamatan orang lain secara individual atau masyarakat;
e. Kepentingan pemeliharaan kesehatan, pengobatan, penyembuhan, dan perawatan pasien;
f. Permintaan pasien itu sendiri;
g. Kepentingan administratif, pembayaran asuransi, atau jaminan pembiayaan kesehatan; dan/atau
h. Kepentingan lain yang diatur dalam peraturan perundang-undangan.

Permenkes 24/2022 berperan sebagai panduan teknis pelaksanaan penyimpanan dan pemanfaatan Rekam Medis Elektronik (RME). Regulasi ini mengatur standar interoperabilitas antar sistem agar data pasien dapat digunakan lintas fasilitas kesehatan tanpa mengorbankan keamanan dan integritasnya. Permenkes ini juga mengatur bahwa data rekam medis harus disimpan minimal selama 25 tahun dan diakses hanya oleh tenaga medis yang berwenang. Prinsip *privacy by design dan privacy by default* menjadi dasar dalam penyusunan sistem RME, memastikan bahwa perlindungan privasi menjadi bagian dari desain sistem sejak awal, bukan hanya tambahan administratif di akhir proses.

Penerapan ketiga regulasi ini sebenarnya telah sangat menjaga perlindungan hukum terhadap data pribadi pasien, namun muncul tantangan baru di era digitalisasi kesehatan, seperti integrasi *big data*, penggunaan *machine learning* untuk prediksi diagnosis, serta kolaborasi lintas sektor antara pemerintah, rumah sakit, dan perusahaan teknologi. Oleh karena itu, prinsip-prinsip bioetika seperti non-maleficence*, beneficence, respect for autonomy*, dan *justice* harus terus menjadi landasan dalam pengambilan keputusan. Perlindungan terhadap kerahasiaan pasien bukan hanya soal kepatuhan hukum, tetapi juga bentuk penghormatan terhadap nilai kemanusiaan dan kepercayaan yang menjadi dasar hubungan dokter-pasien.

Ketiga regulasi (UU PDP, UU Kesehatan, dan Permenkes 24/2022 menunjukkan keselarasan prinsip, namun belum sepenuhnya terintegrasi secara operasional. Walaupun nampak *Normative coherence* ada kesamaan pandangan mengenai hak kerahasiaan pasien dan kewajiban pengendali data. Namun ketika ketiga ruglasi ini diterapkan muncul permasalahan hukum juga, antara lain:

1. Tidak adanya standar nasional tunggal untuk keamanan teknis dan audit akses di fasilitas kesehatan.
2. Ketiadaan mekanisme pelaporan insiden kebocoran data yang baku serta sanksi administratif di Permenkes 24/2022.
3. Belum sinkronnya otoritas pengawas antara Kementerian Kesehatan dan Kementerian Kominfo dalam penegakan pelanggaran di sektor kesehatan.

Tata kelola data yang baik (*good data governance*) harus mengutamakan transparansi, akuntabilitas, dan keadilan distributif. Setiap inovasi berbasis data, baik

untuk penelitian, kebijakan, maupun pelayanan publik, perlu memastikan bahwa manfaatnya dirasakan secara merata oleh seluruh lapisan masyarakat tanpa memperbesar kesenjangan digital. Pengawasan berlapis melalui komite etik, unit perlindungan data di fasilitas kesehatan, serta audit independen menjadi kunci agar sistem tetap berjalan sesuai prinsip etika dan hukum. Dengan demikian, integrasi UU Kesehatan, UU PDP, dan Permenkes 24/2022 tidak hanya menjadi kerangka normatif, tetapi juga fondasi menuju transformasi digital kesehatan yang etis, aman, dan berorientasi pada kesejahteraan manusia.

Berikut Table perbandingan regulasi perlindungan data kesehatan antara Indonesia, Uni Eropa (GDPR), dan Amerika Serikat (HIPAA):

Tabel 1. perbandingan regulasi perlindungan data kesehatan antara Indonesia, Uni Eropa (GDPR), dan Amerika Serikat (HIPAA)

No	**Aspek / Regulasi**	**Indonesia (UU PDP & Permenkes)**	**Uni Eropa (GDPR)**	**Amerika Serikat (HIPAA)**
1	**Kategori data**	Mengatur data pribadi umum dan sensitif, termasuk data kesehatan sebagai data sensitif yang memerlukan perlindungan lebih ketat.	GDPR mengklasifikasikan *health data* sebagai *special category* yang memerlukan perlindungan ekstra.	HIPAA melindungi *Protected Health Information (PHI)* yang mencakup data medis dan identifikasi pasien.
2	**Dasar pemrosesan**	Harus ada dasar hukum yang jelas, termasuk persetujuan eksplisit, kewajiban hukum, keselamatan pasien; data sensitif harus lebih diproteksi.	GDPR mensyaratkan *explicit consent* untuk *special category* data atau dasar sah lain seperti kewajiban hukum & kepentingan kesehatan umum.	HIPAA mengizinkan pemrosesan PHI tanpa persetujuan untuk tujuan perawatan, pembayaran, atau operasi kesehatan tertentu.
3	**Hak subjek data**	Hak akses, koreksi, pembatasan, penghapusan, menarik	Hak luas subjek data termasuk akses, koreksi, hapus, portabilitas,	Fokus pada hak akses dan amandemen PHI; hak penghapusan

		persetujuan – mirip prinsip GDPR meskipun implementasi masih berkembang.	serta penarikan persetujuan.	tidak seterang di GDPR.
4	**Standar keamanan**	Mensyaratkan enkripsi, kontrol akses, audit, dan SOP teknis sesuai Permenkes untuk RME.	GDPR mengharuskan tindakan teknis & organisasional sesuai risiko, termasuk pseudonimisasi dan enkripsi.	HIPAA menetapkan *Security Rule* dengan kontrol administratif, fisik, teknis untuk ePHI.
5	**Akuntabilitas & dokumentasi**	SOP institusi, peta alur data, peninjauan audit internal, bukti pelatihan & pelaporan insiden.	GDPR mensyaratkan dokumentasi dasar hukum, *Data Protection Impact Assessment*, dan bukti kepatuhan.	HIPAA memerlukan audit trail, kebijakan internal, dan pelatihan berkala.
6	**Penggunaan untuk riset & AI**	Diatur dengan prinsip minimisasi, deidentifikasi, dasar hukum yang jelas, persetujuan eksplisit.	GDPR mensyaratkan deidentifikasi atau dasar kuat lain sebelum penggunaan data *special category* untuk riset.	HIPAA membolehkan *Limited Data Set* untuk riset dengan perjanjian pengolahan data.
7	**Sanksi/Penalti**	Sanksi administratif dan pidana, denda signifikan diatur dalam UU PDP.	Denda hingga €20 juta atau ~4 % omzet global, tergantung mana yang lebih tinggi.	Denda finansial & sanksi hukum, dikelola oleh kantor OCR Dept. of HHS.
8	**Ruang lingkup & yurisdiksi**	Berlaku di Indonesia; UU PDP dapat mengekspor kewajiban ke entitas luar yang memproses data warga Indonesia.	Berlaku untuk organisasi di mana pun selama memproses data pribadi warga Uni Eropa.	Berlaku di AS untuk entitas yang menangani PHI; tidak se-ekstrateritorial GDPR.

Berdasarkan perbandingan regulasi perlindungan data kesehatan antara Indonesia, Uni Eropa, dan Amerika Serikat, dapat disimpulkan bahwa Indonesia telah memiliki kerangka hukum yang secara normatif sejalan dengan standar internasional melalui UU PDP dan UU Kesehatan, khususnya dalam pengakuan data kesehatan sebagai data sensitif dan penguatan hak subjek data. Namun, dibandingkan dengan *General Data Protection Regulation* di Uni Eropa yang menekankan prinsip akuntabilitas, penilaian dampak perlindungan data, serta sanksi administratif yang tegas dan terukur, serta *Health Insurance Portability and Accountability Act* di Amerika Serikat yang memiliki standar keamanan teknis dan mekanisme penegakan sektoral yang operasional, regulasi di Indonesia masih menunjukkan kelemahan pada aspek standar teknis nasional yang seragam, mekanisme audit independen, pelaporan insiden kebocoran data, dan kejelasan koordinasi otoritas pengawas lintas sektor. Perbedaan ini menunjukkan bahwa tantangan utama Indonesia bukan terletak pada kekosongan norma, melainkan pada tahap implementasi dan integrasi operasional antar regulasi, sehingga diperlukan penguatan instrumen turunan, penegasan kewenangan pengawasan, serta adopsi praktik terbaik internasional seperti *Data Protection Impact Assessment dan privacy by design* agar perlindungan data kesehatan pasien dapat berjalan efektif, konsisten, dan mampu menjaga kepercayaan publik di era transformasi digital layanan kesehatan.

B.2. Perlindungan Hukum Penggunaan Data Kesehatan

Perlindungan hukum data kesehatan berangkat dari pengakuan bahwa informasi klinis bersifat sangat sensitif sehingga transformasi digital pascapandemi melalui *telehealth* rekam medis elektronik dan integrasi antar fasilitas harus diimbangi dengan penerapan terpadu aturan hukum tata kelola serta pengendalian teknis dan organisasional guna mencegah kebocoran akses tidak sah dan pelebaran tujuan pemrosesan serta menjaga keselamatan pasien dan kepercayaan publik (Theodos & Sittig, 2020). Perlindungan data yang efektif menuntut akuntabilitas yang dapat dibuktikan melalui pemetaan alur data pencatatan dasar hukum pelatihan berkala dan audit akses karena bukti empiris menunjukkan ketahanan fasilitas kesehatan terhadap insiden siber lebih ditentukan oleh proses organisasi dan evaluasi berkelanjutan dibanding ketergantungan pada alat keamanan semata. Perlindungan data kesehatan yang efektif menuntut dasar keabsahan pemrosesan yang jelas, persetujuan yang benar-benar dipahami atau dasar hukum lain yang sah, serta pemetaan dan dokumentasi alur data yang dapat diaudit dengan pengendalian tambahan sesuai tingkat risiko (Keesara et al., 2020).

Perlindungan hukum menghendaki kontrol yang berjalan sehari-hari dimana didalmnya meliputi otentikasi kuat, manajemen identitas, segmentasi jaringan, enkripsi *at rest/in transit*, peninjauan log, cadangan terenkripsi yang terpisah, pembaruan sistem, uji kerentanan, uji penetrasi, serta latihan respons insiden (*table-top exercise*). Bukti organisasi rumah sakit menunjukkan kombinasi kebijakan dan proses yang disiplin menurunkan frekuensi serta dampak insiden (Keesara et al., 2020). Pertukaran data yang

cepat dan aman meningkatkan kesinambungan asuhan, efisiensi rujukan, dan keselamatan pasien (Gunawan & Christianto, 2020). Audit mutu, pendidikan klinik, kebijakan berbasis data, dan pengembangan AI memerlukan tujuan yang spesifik, dasar hukum yang jelas, prinsip minimisasi, serta deidentifikasi atau pseudonimisasi, karena tanpa pengaturan tersebut berisiko terjadi pelebaran tujuan dan ketidakadilan algoritmik, sehingga dokumentasi protokol, pengawasan etik independen, dan kanal audit harus tersedia sebelum penggunaan data di luar pelayanan langsung (Parsaoran & Sitompul, 2023).

Etika kecerdasan buatan dalam layanan kesehatan menempatkan keselamatan pasien, keadilan, privasi, dan akuntabilitas sebagai landasan utama, dengan penggunaan data yang harus bertujuan jelas dan didasarkan pada persetujuan yang benar-benar dipahami (Darmadi et al., 2025). Uji dampak perlindungan data dan dokumentasi pemrosesan yang jelas memungkinkan pemetaan risiko dan penelusuran akuntabilitas sementara pengujian bias kesetaraan kinerja dan keamanan model disertai transparansi serta pengawasan berkelanjutan memastikan kecerdasan buatan berfungsi sebagai pendukung keputusan klinis dengan tanggung jawab akhir tetap pada profesional kesehatan (Keesara et al., 2020).

Perlindungan hukum yang berorientasi pasien menuntut transparansi lokasi penyimpanan, retensi, pihak yang mengakses, serta mekanisme pengaduan. Akses pasien ke rekam medis elektronik dikaitkan dengan peningkatan keterlibatan klinis dan kepatuhan; sistem perlu menyediakan akses yang aman namun mudah digunakan, termasuk prosedur untuk koreksi data, pembatasan pemrosesan, hingga penghapusan sesuai syarat hukum (E. Li et al., 2022). Transformasi digital kesehatan harus diukur dari peningkatan keselamatan pasien melalui persetujuan yang benar-benar dipahami dan tata kelola data yang dapat diaudit, berakses ketat, patuh pada prinsip minimisasi dan deidentifikasi, serta didukung pelaporan insiden, pembagian peran yang jelas, dan pengaturan pihak ketiga guna menjaga keselamatan, keadilan dan kepercayaan pasien.

C. Prinsip Etika Penggunaan Data Kesehatan

a) Respect for Autonomy

Respect for autonomy menempatkan pasien sebagai pengambil keputusan utama atas data kesehatan dirinya. Dalam kerangka bioetik klasik, otonomi berdiri sejajar dengan beneficence, non-maleficence, dan justice; dari asas ini lahir kewajiban *informed consen*t, kejujuran informasi, serta kerahasiaan. Artinya, setiap pengumpulan, penyimpanan, pemrosesan, dan pertukaran data hanya etis bila pasien memahami tujuan, konsekuensi, serta alternatif yang tersedia, lalu memberi persetujuan secara bebas tanpa paksaan (Parsaoran & Sitompul, 2023). Landasan ini tidak hanya bernilai moral, tetapi juga menjadi prasyarat legitimasi praktik klinis di era digital, terutama dalam sistem rekam medis elektronik yang mengedepankan hak pasien atas persetujuan dan kontrol atas data pribadi mereka (Varkey, 2021). Etika pengelolaan data kesehatan bertumpu pada prinsip respect for autonomy dan keselamatan pasien, sehingga setiap

pemrosesan data harus berpusat pada manusia serta didukung pendekatan etis yang konkret, terukur, dan dapat diaudit agar inovasi digital memberi manfaat klinis tanpa mengabaikan hak dan keadilan pasien. Percepatan digitalisasi pascapandemi meningkatkan koordinasi layanan sekaligus kerentanan etis, sehingga penggunaan data perlu disertai pengelolaan risiko yang proporsional melalui tujuan yang jelas, minimisasi data, pembatasan akses, dan jejak audit yang mudah ditelusuri (Ftouni et al., 2022).

b) Beneficence

Asas *beneficence* menuntut setiap penggunaan data kesehatan menghasilkan manfaat nyata bagi pasien, tenaga kesehatan, dan sistem layanan. Manfaat yang dimaksud bukan sekadar efisiensi administratif, tetapi perbaikan keselamatan, mutu klinis, pengalaman pasien, serta hasil kesehatan jangka pendek dan jangka panjang. Dalam kerangka ini, pengumpulan dan pemrosesan data harus selalu terikat pada tujuan klinis yang jelas, proporsional dengan kebutuhan, dan dapat dipertanggungjawabkan kepada pasien sebagai penerima manfaat utama (Goldschmitt et al., 2025).

c) Non-Maleficence

Prinsip non-maleficence menekankan kewajiban untuk mencegah segala bentuk kerugian terhadap kerahasiaan, integritas, dan ketersediaan data. Nilai ini diwujudkan melalui penerapan *privacy by design* dan *privacy by default*, yang mencakup langkah-langkah operasional seperti minimisasi data, pembatasan tujuan penggunaan, enkripsi saat penyimpanan dan transmisi, pengendalian akses berbasis peran, serta audit log secara berkala. Kajian mengenai tata kelola digital menunjukkan bahwa pendekatan tersebut bukan sekadar norma etis, melainkan strategi efektif untuk menekan risiko akses tidak sah, kebocoran data, dan penyalahgunaan tujuan pemrosesan (Tapuria et al., 2021).

d) *Justice* (Keadilan)

Asas keadilan menuntut akses perlindungan yang setara, hasil klinis yang adil, dan alokasi sumber daya yang tidak diskriminatif. Prinsip keadilan menekankan pentingnya pemerataan manfaat dan beban dalam pemanfaatan data kesehatan. Setiap individu berhak memperoleh perlindungan yang sama terhadap kerahasiaan dan keamanan datanya, tanpa diskriminasi berdasarkan status sosial, ekonomi, atau kondisi kesehatan. Penerapan prinsip ini menuntut transparansi dalam pengumpulan, pemrosesan, serta distribusi hasil analisis data agar tidak menimbulkan ketimpangan akses maupun bias algoritmik. Literatur etika digital menunjukkan bahwa tata kelola data yang berkeadilan memastikan inovasi berbasis data memberikan manfaat secara setara bagi seluruh kelompok masyarakat, sekaligus mencegah eksploitasi data dari populasi yang rentan atau kurang terwakili (Goldschmitt et al., 2025).

Kesimpulan

Kajian ini menegaskan bahwa perlindungan hukum data kesehatan pasien di era digital harus mengintegrasikan kerangka hukum nasional dengan prinsip etika kedokteran, yang saat ini bertumpu pada UU Kesehatan, UU PDP, dan Permenkes 24/2022 sebagai landasan normatif tata kelola data yang aman dan akuntabel, namun masih menghadapi kelemahan dibandingkan pengaturan di Uni Eropa melalui GDPR dan di Amerika Serikat melalui HIPAA akibat perbedaan standar teknis, ketiadaan sanksi dan mekanisme pengaduan yang jelas, serta belum sinkronnya kewenangan antar kementerian. Oleh karena itu, efektivitas perlindungan sangat bergantung pada penerapan operasional prinsip otonomi, kemanfaatan, tidak merugikan, dan keadilan melalui kebijakan internal, audit independen, penilaian dampak perlindungan data, serta pendidikan etika digital, sehingga diperlukan pedoman nasional yang adaptif, penegasan otoritas penegakan hukum, dan pendekatan berbasis risiko guna meningkatkan kepercayaan publik dan mendukung transformasi layanan kesehatan yang berkeadilan di Indonesia.

Daftar Bacaan

Peraturan Perundang-undangan :

Kementerian Kesehatan Republik Indonesia. (2023). Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan. Jakarta: Kementerian Kesehatan RI.

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis. Jakarta: Kementerian Kesehatan RI.

Undang – Undang Perlindungan Data Pribadi No. 27 Tahun 2022

Jurnal :

Ali, O., & Osmanaj, V. (2020). The role of government regulations in the adoption of cloud computing: A case study of local government. Computer Law and Security Review, 36. https://doi.org/10.1016/j.clsr.2020.105396

Darmadi, E. Y., Andriani Fauziah, Y., Deriano Alvin, J., Alexandra Mayfrila, A., & Cyntia, W. (2025). Ethical And Legal Aspects Of Artificial Intelligence In Oral Health (Vol. 13, Issue 4). https://ejournal.uika-bogor.ac.id/index.php/Hearty/issue/archive

Fauziah, Y. A., Agustin Wahjuningrum, D., Edwin Sutikno, A., Agus Susanto, D., Wahjudianto, N., & Goenharto, A. (2024). Ethical and Legal Aspect of Digital Dentistry in Conservative Dental Practice. In Journal of International Dental and Medical Research (Vol. 17, Issue 4). http://www.jidmr.com

Fauziah, Y. A., Alhadad, H., & Susanto, D. A. (2025). Dental Malpractice and Criminal Liability : A Review of Law No. 17 of 2023 on Health. Jurnal Hukum Dan Etika Kesehatan, 5(1).

Fauziah, Y. A., Alhadad, H., & Utama, Y. P. (2024). Etika dan Tantangan Penggunaan Kecerdasan Buatan Dalam Kedokteran Gigi. Jurnal Hukum Dan Etika Kesehatan, 4(2).

Fauziah, Y. A., Darmadi, E. Y., Khoironi, E., & Yudianto, A. (2025). The Role of Cone Beam Computed Tomographic (CBCT) in Odontology Forensic for Forensic Identification. Indonesian Journal of Legal and Forensic Sciences (IJLFS), 14(2), 87–94. https://doi.org/10.24843/IJLFS.2024.v14.i02.p02

Fauziah, Y. A., Wahjuningrum, D. A., Darmadi, E. Y., & Adityatama, A. P. (2024). Innovation in Dental Conservation and Their Impact on Forensic Odontology. Conservative Dentistry Journal, 14(2), 42–46. https://doi.org/10.20473/cdj.v14i2.2024.42-46

Ftouni, R., AlJardali, B., Hamdanieh, M., Ftouni, L., & Salem, N. (2022). Challenges of Telemedicine during the COVID-19 pandemic: a systematic review. BMC Medical Informatics and Decision Making, 22(1). https://doi.org/10.1186/s12911-022-01952-0

Goldschmitt, M., Gleim, P., Mandelartz, S., Kellmeyer, P., & Rigotti, T. (2025). Digitalizing informed consent in healthcare: a scoping review. BMC Health Services Research, 25(1). https://doi.org/10.1186/s12913-025-12964-7

Gunawan, T. S., & Christianto, G. M. (2020). Rekam Medis/Kesehatan Elektronik (RMKE): Integrasi Sistem Kesehatan. Jurnal Etika Kedokteran Indonesia, 4(1). https://doi.org/10.26880/jeki.v4i1.43

Ho, C. H. (2024). Secondary Use of Health Data for Medical AI: A Cross-Regional Examination of Taiwan and the EU. Asian Bioethics Review, 16(3), 407–422. https://doi.org/10.1007/s41649-024-00279-4

Jungkunz, M., Köngeter, A., Mehlis, K., Winkler, E. C., & Schickhardt, C. (2021). Secondary use of clinical data in data-gathering, non-interventional research or learning activities: Definition, types, and a framework for risk assessment. Journal of Medical Internet Research, 23(6). https://doi.org/10.2196/26631

Keesara, S., Jonas, A., & Schulman, K. (2020). Covid-19 and Health Care's Digital Revolution. New England Journal of Medicine, 382(23).

https://doi.org/10.1056/nejmp2005835

Li, E., Clarke, J., Ashrafian, H., Darzi, A., & Neves, A. L. (2022). The Impact of Electronic Health Record Interoperability on Safety and Quality of Care in High-Income Countries: Systematic Review. In Journal of Medical Internet Research (Vol. 24, Issue 9). https://doi.org/10.2196/38144

Li, Z., Merrell, M. A., Eberth, J. M., Wu, D., & Hung, P. (2023). Successes and Barriers of Health Information Exchange Participation Across Hospitals in South Carolina From 2014 to 2020: Longitudinal Observational Study. JMIR Medical Informatics, 11. https://doi.org/10.2196/40959

Nusantara, A. H. S., Umam, I. K., & Lubis, M. (2024). Jaminan Informasi dan Keamanan yang Lenih Baik: Studi Kasus BPJS Kesehatan. *Nuansa Informatika*, *18*(2), 120–127.

Parsaoran, A., & Sitompul, H. (2023). Penggunaan Rekam Medis Elektronik Untuk Pasien Rawat Jalan Di Fasilitas Kesehatan Indonesia : Literature Review. Jurnal Ilmiah Multidisipline, 37(2).

Solimini, R., Busardò, F. P., Gibelli, F., Sirignano, A., & Ricci, G. (2021). Ethical and legal challenges of telemedicine in the era of the covid-19 pandemic. In Medicina (Lithuania) (Vol. 57, Issue 12). MDPI. https://doi.org/10.3390/medicina57121314

Tapuria, A., Porat, T., Kalra, D., Dsouza, G., Xiaohui, S., & Curcin, V. (2021). Impact of patient access to their electronic health record: systematic review. Informatics for Health and Social Care, 46(2). https://doi.org/10.1080/17538157.2021.1879810

Theodos, K., & Sittig, S. (2020). Health Information Privacy Laws in The Digital Age: HIPAA Doesn't Apply.

Varkey, B. (2021). Principles of Clinical Ethics and Their Application to Practice. In Medical Principles and Practice (Vol. 30, Issue 1). https://doi.org/10.1159/000509119

Website :

Kompas.com. (2021, May 21). Kemenkominfo duga 279 juta data penduduk yang bocor identik dengan data BPJS Kesehatan. https://nasional.kompas.com/read/2021/05/21/15192491/kemenkominfo-duga-279-juta-data-penduduk-yang-bocor-identik-dengan-data-bpjs

Kompas.com. (2021, June 4). Polri: Diduga keras data kependudukan BPJS Kesehatan bocor. https://nasional.kompas.com/read/2021/06/04/06300041/polri--diduga-keras-data-kependudukan-bpjs-kesehatan-bocor